

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-61277

(43) 公開日 平成10年(1998) 3月3日

(51) IntCl ⁶	識別記号	庁内整理番号	F I	技術表示箇所
E 0 5 B 49/00			E 0 5 B 49/00	K
B 6 0 R 25/00	6 0 6		B 6 0 R 25/00	6 0 6
E 0 5 B 47/00			E 0 5 B 47/00	U
65/19			65/19	B
65/20			65/20	

審査請求 未請求 請求項の数 6 O L (全 6 頁) 最終頁に続く

(21) 出願番号 特願平8-222044

(22) 出願日 平成8年(1996) 8月23日

(71) 出願人 000004260

株式会社デンソー

愛知県刈谷市昭和町1丁目1番地

(72) 発明者 中野 彰夫

愛知県刈谷市昭和町1丁目1番地 日本電
装株式会社内

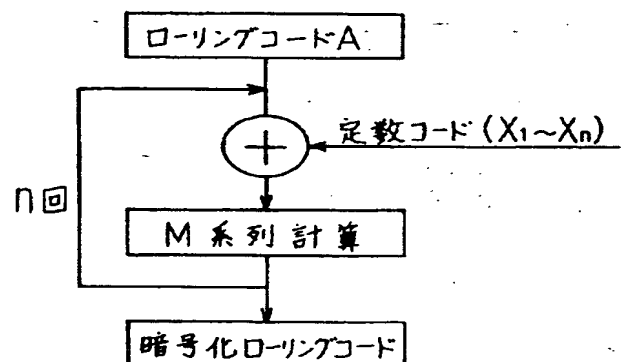
(74) 代理人 弁理士 磯水 裕彦

(54) 【発明の名称】 遠隔操作装置

(57) 【要約】

【課題】 設計者といえども送信コードの解読ができないようにすること。

【解決手段】 ローリングコード変更テーブル中の定数コードXとローリングコードAとの排他的論理和の演算、および周知のM系列演算をn回繰り返すにより、ローリングコードAが暗号化され、暗号化ローリングコードが生成される。なお、k回目の排他的論理和の演算の際には、車両固有のキーコードが定数コード X_k として用いられることになるので、k回目の排他的論理和の演算の方法は車両毎に異なることになり、しいては、暗号化の方法が車両毎に異なることになる。また、キーコードは車両の製造工程においてEEPROM19に書込まれるようになっているので、キーコードを製造工程まで秘密にしておけば、設計者であっても、ローリングコードAの暗号化は見破られることない。



【特許請求の範囲】

【請求項１】 固有の識別情報がコード化されたＩＤコードと、このＩＤコードを暗号化するために用いられるローリングコードとの２つのコードを含む送信コードを送信する送信機と、前記送信機から送信された前記送信コードを受信して、この送信コードから前記ＩＤコードを復元し、復元されたＩＤコードに基づいて制御の対象を作動させる指令を出力する受信機とを備えた遠隔操作装置において、
前記送信機は、
各々の装置固有に定められたキーコードを格納した格納手段と、
前記キーコードに基づいて前記ローリングコードを暗号化して暗号化ローリングコードを生成する生成手段と、
前記暗号化ローリングコードを用いて前記ＩＤコードを暗号化する暗号化手段とを備えることを特徴とする遠隔操作装置。

【請求項２】 前記送信機内に互いに異なる定数コードが設定されたローリングコード変更テーブルを備え、前記生成手段は、前記ローリングコードと前記ローリングコード変更テーブルに設定された前記定数コードとを論理演算することにより暗号化ローリングコードを生成するものであることを特徴とする請求項１記載の遠隔操作装置。

【請求項３】 前記生成手段は、前記ローリングコードと前記定数コードとを論理演算した後に、Ｍ系列計算を行うことにより暗号化ローリングコードを生成するものであることを特徴とする請求項２記載の遠隔操作装置。

【請求項４】 前記生成手段は、前記論理演算と前記Ｍ系列計算を複数回繰り返して行うことにより、暗号化ローリングコードを生成するものであることを特徴とする請求項３記載の遠隔操作装置。

【請求項５】 前記格納手段は不揮発性記憶媒体を含み、前記キーコードは装置の製造工程において前記不揮発性記憶媒体に記憶されるものであることを特徴とする請求項２記載の遠隔操作装置。

【請求項６】 前記キーコードは、前記不揮発性記憶媒体から読み出され、前記ローリングコード変更テーブルに設定された定数コードの少なくとも１つに設定されるものであることを特徴とする請求項５記載の遠隔操作装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】 本発明は、車両のワイヤレスドアロック制御装置等に用いられる遠隔操作装置に関するものである。

【０００２】

【従来の技術】 従来、車両のワイヤレスドアロック制御装置に採用されるような遠隔操作装置では、不正防止の観点から、送信機から送信される送信コードを解読され

ないように暗号化することがなされている。例えば、特開平８－１０２９８２号公報に開示された装置では、送信コードが送信される毎に所定の順序で変更されるローリングコードを用いて送信コードを暗号化している。

【０００３】

【発明が解決しようとする課題】 しかしながら、上記公報に開示された装置では、ローリングコードの変更順序は予め設定されているものであるため、この変更順序を設定した者、すなわち設計者であれば暗号化された送信コードの解読が可能であり、十分な暗号化がなされているとは言えなかった。

【０００４】 そこで本発明は上記問題点を鑑みてなされたものであり、解読の難しさを向上し、設計者といえども送信コードの解読を困難とした遠隔操作装置を提供することを目的とするものである。

【０００５】

【課題を解決するための手段】 上記目的を達成するため請求項１記載の発明では、送信機は、各々の装置固有に定められたキーコードに基づいてローリングコードを暗号化して暗号化ローリングコードを生成し、暗号化ローリングコードを用いてＩＤコードを暗号化する。よって、装置固有に定められたキーコードさえ秘密にしておけば、暗号化ローリングコード生成のアルゴリズムを設定したものであっても、ローリングコードの暗号化の解読は困難となるので、送信コードの解読の難かしさが向上し、ユーザ以外の不正な使用を防止することができる。

【０００６】 請求項４記載の発明では、論理演算とＭ系列計算を複数回繰り返して行うことにより暗号化ローリングコードを生成しているので、一層ローリングコードの暗号化の解読は困難なものとなる。請求項５記載の発明では、キーコードは、装置の製造工程において不揮発性記憶媒体に記憶されるようにしているので、装置の製造工程までキーコードを秘密にしておく、あるいは製造工程でランダムにキーコードを設定すれば、ローリングコードの暗号化は解読されることはない。

【０００７】

【発明の実施の形態】 以下、本発明の実施の形態を図面を用いて説明する。

【第１の実施形態】 図１は、本発明の遠隔操作装置を車両用のワイヤレスドアロック制御を行う装置に採用した際の第１の実施形態の構成を示すブロック図である。

【０００８】 図１において、１は送信機であり、この送信機１は、それぞれ異なった機能（例えば、ドアロック、トランクの開閉、シートポジションの設定等）を遠隔作動させるためのスイッチ１２－１、１２－２、…、１２－ｎが設けられており、そのスイッチ操作はマイクロプロセッサ１１に入力されるように構成されている。このマイクロプロセッサ１１は、ＥＥＰＲＯＭ１９が接続されており、このＥＥＰＲＯＭ１９には、送信機１固

有のIDコードAと、送信コードが送信される毎に所定の順序で変化するローリングコードAと、車両固有のキーコードとが記憶されている。これらのIDコードA、ローリングコードA、およびキーコードは、車両の製造工程においてEEPROM19に記憶させるものである。また、マイクロプロセッサ11中には、ローリングコードAを暗号化するためのローリングコード変更テーブルと、送信コード生成のための情報とがアルゴリズムとして記憶されている。ローリングコード変更テーブルは、図3に示すように構成されている。図3中、 x_1 番地 $\sim x_n$ 番地には、各々異なるjビットからなる定数コード $X_1 \sim X_n$ が設定されている。このうち、 x_k 番地($1 \leq k \leq n$)には、EEPROM19から車両固有のキーコードが読み出され、定数コード X_k として設定されるようになっている。さらに、マイクロプロセッサ11には、発信回路14及びFM変調回路15が接続されており、マイクロプロセッサ11にて生成された送信コードをFM変調して微弱電波として放射するように構成されている。

【0009】一方、受信機2には、送信機1から放射された微弱電波を復調する受信回路が設けられており、この受信回路は高周波増幅回路25、局部発振器24、ミキサ回路26、中間周波増幅回路27、復調回路28によって構成され、その復調された出力信号がマイクロプロセッサ21に入力されるように構成されている。なお、このマイクロプロセッサ21は、予め定められた所定の処理に基づいて、復調された出力信号からIDコードAとローリングコードAを復元する。また、マイクロプロセッサ21にはEEPROM29が接続されており、このEEPROM29は受信機2固有のIDコードBと、前回受信した送信コードに含まれていたローリングコードAに対応したローリングコードBと、車両固有のキーコードとが記憶されている。また、マイクロプロセッサ21中には、ローリングコードAを復元するためのローリングコード変更テーブル(図3と同じ)と、出力信号からIDコードAとローリングコードAを復元するための情報とがアルゴリズムとして記憶されている。そして、マイクロプロセッサ21には、駆動回路23-1、23-2、 \dots 、23-nを介して、制御対象となる3-1、3-2、 \dots 、3-n(例えば、ドアロック、トランクの開閉、シートポジションの設定等を行うアクチュエーター)が接続されており、この制御対象となる3-1、3-2、 \dots 、3-nはマイクロプロセッサ21からの信号に応じて作動するように構成されている。

【0010】次に、上記構成の送信機1及び受信機2の動作を図2に示すフローチャートに基づき説明する。なお、このフローチャートはそれぞれ送信機1、受信機2に設けられたマイクロプロセッサ11、21により実行される処理を示す。まず、送信機1の動作を説明する。

ステップ10にて、スイッチ12-1 \sim 12-nのいずれかが操作されたと判断するまで待機し、スイッチが操作されたと判断した時点でステップ20に移行する。ステップ20にて、ローリングコードAの更新を行う。このローリングコードAはjビットからなる変数で、送信が行われる毎に+1変化するものとする。なお、送信が行われる毎に+1変化するとしているがこれに限らず、所定の規則に従って変化するものであればよい。

【0011】次に、ステップ30にて、ローリングコード変更テーブルを用いてローリングコードAを暗号化することにより暗号化ローリングコードを生成する。この暗号化ローリングコードの生成方法を図3、および図4を用いて説明する。まず、図3に示すローリングコード変更テーブル中の x_1 番地の定数コード X_1 とローリングコードAとの排他的論理和の演算を行う。次に、周知のM系列演算を行う。その後、 x_2 番地以降の定数コードXを用いた排他的論理和の演算とM系列計算をn回繰り返す。この排他的論理和の演算とM系列計算の繰り返しにより、ローリングコードAが暗号化され、暗号化ローリングコードが生成される。なお、k回目の排他的論理和の演算の際には、車両固有のキーコードが定数コード X_k として用いられることになるので、k回目の排他的論理和の演算の方法は車両毎に異なることになり、しいては、暗号化の方法が車両毎に異なることになる。また、キーコードは車両の製造工程においてEEPROM19に書込まれるようになっているので、キーコードを製造工程まで秘密にしておく、あるいは製造工程でランダムにキーコードを設定すれば、図4に示すロジックを考えた設計者であっても、ローリングコードAの暗号化は解読されることはない。

【0012】次に、ステップ40にて、暗号化ローリングコード、EEPROM19に記憶されているIDコードA、および機能コードとを用いて送信コードを生成する。機能コードとは、制御対象となる3-1、3-2、 \dots 、3-nを作動させるためのコードである。そして、ステップ50にて、ステップ40で生成された送信コードをFM変調回路15に出力する。これにより、送信コードはFM変調されて微弱電波として送信機1外部に放射される。送信コードを送信する。なお、送信コードの生成については、前述した特開平8-102982号公報に詳しいのでそちらを参照されたい。

【0013】以上の一連のステップは、操作スイッチが一回押された場合の送信機1側の処理であって、再び操作スイッチが押された場合は、ステップ20 \sim 50の処理が再度実行され、この場合、ローリングコードは変更されることになる。次に、受信機2の動作を説明する。ステップ110にて、送信機1からの送信コードが受信されるまで待機し、送信コードが受信された時点でステップ120に移行する。ステップ120では、送信コードからIDコードAとローリングコードAとを復元す

る。

【0014】次に、ステップ130にて、EEPROM 29に記憶されているIDコードBとステップ120で復元された送信コードのIDコードAとが一致するか否かを判定する。一致すればステップ150に移行し、一致しなければステップ110にて待機状態となる。さらに、ステップ140にて、ステップ120で復元されたローリングコードAと、EEPROM 29に記憶されているローリングコードBとを比較し、復元されたローリングコードAがローリングコードBに対し所定の範囲内にあるか否かを判定する。範囲内であれば、ローリングコードは正しいとしてステップ150に移行し、範囲外であればステップ110にて待機状態となる。このとき、送信機1の送信コードが受信機2側で毎回受信されるのであれば、受信機側で比較判定するローリングコードAは、ローリングコードBの値+1に限定してもよい。しかしながら、送信機1が操作されても受信機側で受信されない場合（いわゆる送信機1のカラ打ち）、送信機1のローリングコードAのみが更新されるため、この場合にも対応できるように許容範囲を定めている。例えば、送信コードから復元したローリングコードAの値 r_i 、EEPROM 29に記憶されているローリングコードBの値 r_{i-1} として、“ $r_{i-1} + 1 \leq r_i \leq r_{i-1} + \alpha$ ”（ α は任意の自然数）であればローリングコードAは正常であると判定する。

【0015】次に、ステップ150にて、送信コードから復元したローリングコードAをEEPROM 29にローリングコードBとして記憶することにより、ローリングコードBを更新する。これによって、送信機1のカラ打ちにより送信機1のローリングコードAのみが更新され、送信機1と受信機2とに設定されるローリングコードに差が生じたとしても、受信機2が送信コードを受信した場合には、送信コードから復元したローリングコードAでローリングコードBを更新するので、送信コード受信後のローリングコードAとローリングコードBは一致することになる。

【0016】さらに、ステップ160にて、送信コードに設定されていた機能コードに対応して、駆動回路23-1、23-2、…、23-nを介して、制御対象となる3-1、3-2、…、3-nを作動させる。なお、この実施形態においては、EEPROM 19、およびローリングコード変更テーブルの x_k 番地が格納手段に相当し、図2のステップ30の処理が生成手段に相当し、図2のステップ40の処理が暗号化手段に相当する。

【0017】【他の実施形態】第1の実施形態では、ローリングコードの暗号化処理は、1回の排他的論理和の演算と1回のM系列計算を1セットとしているが、図5に示すように、1回の排他的論理和の演算と2回のM系列計算を1セットとしてしても良いし、図6に示すように、2回の排他的論理和の演算と2回のM系列計算を1セットとしてしても良い。さらに、図7、8に示すように、1回目のM系列計算が終了した後に、ローリングコードを構成しているjビットの信号の前半部分と後半部分とを入れ替えるようにしても良い。図5～図8の暗号化処理を採用することによって、暗号化ローリングコードの解読が一層困難なものとなる。

【0018】第1の実施形態では、EEPROM 19、29は、マイクロプロセッサ11、12と別体に構成されているが、マイクロプロセッサ11、12に内蔵しても良い。また、第1の実施形態では、キーコードはローリングコード変更テーブルの x_k 番地のみに設定されていたが、複数の番地に設定するようにしても良い。さらに第1の実施形態では、幾つかの機能を作動させる構成としたが、機能を単一のものにすることによって、機能ビットのない応用例を実現することもできる。

【図面の簡単な説明】

【図1】本発明の実施形態の構成を示すブロック図である。

【図2】図1に示す送信機、受信機の動作を表すフローチャートである。

【図3】ローリングコードAを暗号化するためのローリングコード変更テーブルである。

【図4】第1の実施形態におけるローリングコードAを暗号化するためのロジックを説明するための図である。

【図5】他の実施形態におけるローリングコードAを暗号化するためのロジックを説明するための図である。

【図6】他の実施形態におけるローリングコードAを暗号化するためのロジックを説明するための図である。

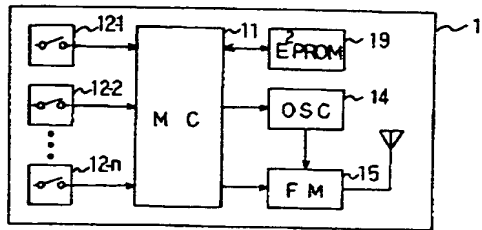
【図7】他の実施形態におけるローリングコードAを暗号化するためのロジックを説明するための図である。

【図8】他の実施形態におけるローリングコードAを暗号化するためのロジックを説明するための図である。

【符号の説明】

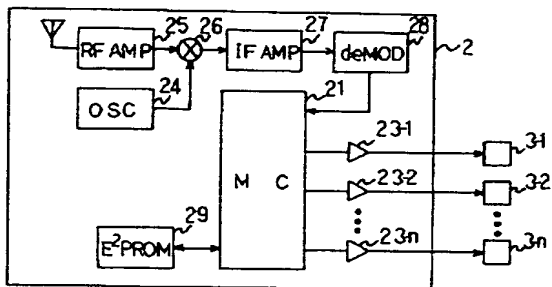
- 1 送信機
- 2 受信機
- 3 アクチュエータ
- 11 マイクロプロセッサ
- 21 マイクロプロセッサ

【図1】

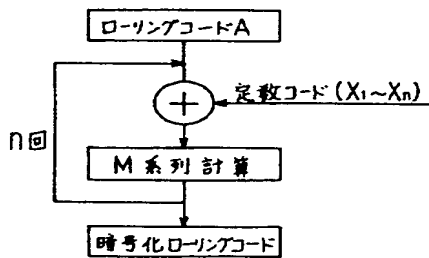


【図3】

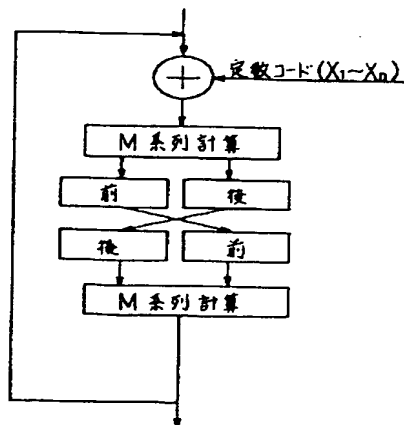
番地	定数コード(ビット)
X ₁	定数コード X ₁
X ₂	定数コード X ₂
...	...
X _k	定数コード X ₃ ← キーコード
...	...
X _n	定数コード X _n



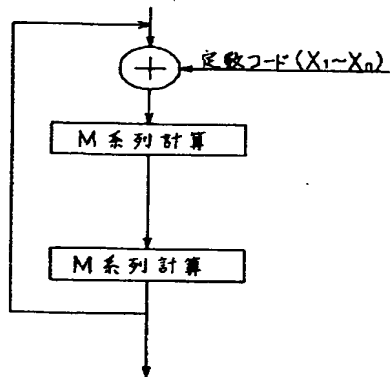
【図4】



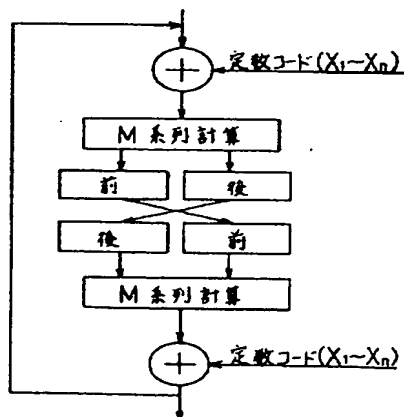
【図7】



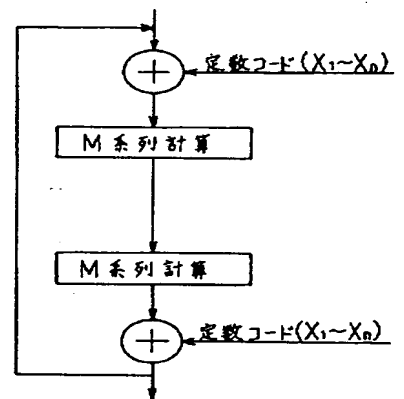
【図5】



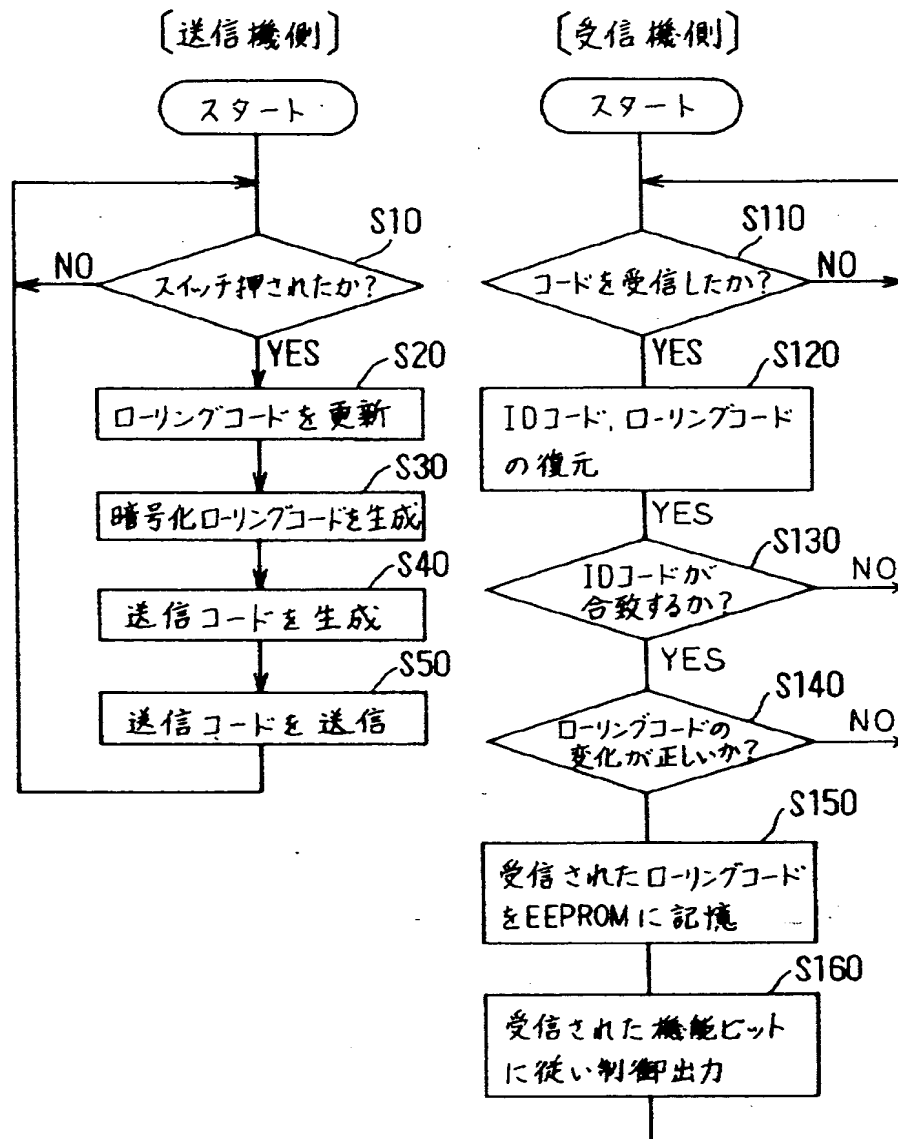
【図8】



【図6】



【図2】



フロントページの続き

(51) Int. Cl. 6
H04Q 9/00

識別記号 弁内整理番号
301
311

FI
H04Q 9/00

技術表示箇所

301B
311N